#4

Dkt. 64498/JPW/PT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Masanori Kusunoki

Serial No.: 09/805,284

Filed : March 13, 2001

For : SYSTEM FOR AUTHENTICATING ACCESS TO A NETWORK, STORAGE MEDIUM, PROGRAM AND METHOD FOR AUTHENTICATING ACCESS TO A NETWORK

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

TRANSMITTAL OF CERTIFIED COPIES OF EARLIER FILED FOREIGN APPLICATIONS AND CLAIM TO PRIORITY PURSUANT TO 35 U.S.C. §119

Applicant submits herewith certified copies of Japanese Patent Application Nos. 2000-069079 and 2001-061999 filed in Japan on March 13, 2000 and March 6, 2001, respectively, and cited in Applicant's Declaration pursuant to 37 C.F.R. §1.63.

Applicant hereby claims the benefit of the March 13, 2000 and March 6, 2001 filing dates pursuant to 35 U.S.C. §119 and 37 C.F.R. §1.55(a).

Respectfully submitted,

Paul Teng

John P. White
Registration No. 28,678
Paul Teng
Registration No. 40,837
Attorneys for Applicant
Cooper & Dunham LLP
1185 Avenue of the Americas
New York, New York 10036
(212) 278-0400

I hereby certify that this paper is being deposited this date with the U.S. Postal Service with sufficient postage as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231.

Paul Teng — July 12, 2001
Paul Teng
Reg. No. 40,837
Date

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　３月１３日

出願番号
Application Number: 特願２０００－０６９０７９

願人
Applicant (s): ヤフー株式会社

CERTIFIED COPY OF PRIORITY DOCUMENT

２００１年　３月２３日

特許庁長官
Commissioner,
Patent Office 及川耕造

【書類名】　特許願
【整理番号】　A000001028
【提出日】　平成12年 3月13日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 17/00
【発明の名称】　アクセス認証システム及びアクセス認証方法
【請求項の数】　7
【発明者】
【住所又は居所】　東京都渋谷区恵比寿１－２４－１６　ピー・アイ・エム株式会社内
【氏名】　楠　正憲
【特許出願人】
【住所又は居所】　兵庫県神戸市中央区港島南町１－５－２
【氏名又は名称】　ピー・アイ・エム株式会社
【代理人】
【識別番号】　100058479
【弁理士】
【氏名又は名称】　鈴江　武彦
【電話番号】　03-3502-3181
【選任した代理人】
【識別番号】　100084618
【弁理士】
【氏名又は名称】　村松　貞男
【選任した代理人】
【識別番号】　100068814
【弁理士】
【氏名又は名称】　坪井　淳
【選任した代理人】
【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　アクセス認証システム及びアクセス認証方法

【特許請求の範囲】

【請求項１】

第１のターミナルサーバを経由してクライアントに第２のターミナルサーバへの接続サービスを行うアクセス認証システムにおいて、

上記第１のターミナルサーバに対して上記クライアントから入力された個別情報に基づいて上記第１のターミナルサーバへの上記クライアントの接続の可否を認証するとともに、上記個人情報の一部を含むクライアントパラメータを所定の規則で符号化した第１のチケットデータを作成し、上記第２のターミナルサーバに転送する第１の認証サーバと、

上記クライアントパラメータの正当性及び上記第１のチケットデータの行使の有無を検証するとともに、上記クライアントパラメータを所定の規則で符号化した第２のチケットデータを作成し、この第２のチケットデータと上記第１のチケットデータとを照合し、上記第２のターミナルサーバへ上記クライアントの接続可否を指示する第２の認証サーバとを備えていることを特徴とするアクセス認証システム。

【請求項２】

上記所定の規則は、一方向関数による要約であることを特徴とする請求項１に記載のアクセス認証システム。

【請求項３】

上記クライアントパラメータには、上記クライアントのＩＤ、アクセス元ＩＰアドレス、上記第１のチケットデータの有効期限のうち少なくとも１つが含められていることを特徴とする請求項１に記載のアクセス認証システム。

【請求項４】

上記第１及び第２の認証サーバにおいて、上記第１及び第２のチケットデータを作成する際に、予め定められた共通の文字列を含めることを特徴とする請求項１に記載のアクセス認証システム。

【請求項５】

上記共通の文字列は、所定のタイミングで変更されるものであることを特徴とする請求項４に記載のアクセス認証システム。

【請求項６】

第１のターミナルサーバを経由してクライアントに第２のターミナルサーバへの接続サービスを行うアクセス認証方法において、

上記第１のターミナルサーバへの上記クライアントの接続の可否を認証する第１の認証ステップと、

上記クライアントから入力された個別情報の少なくとも一部を含むクライアントパラメータを所定の規則で符号化した第１のチケットデータを作成する第１チケットデータ作成ステップと、

上記第２のターミナルサーバに上記クライアントパラメータ及び上記第１のチケットデータを転送するデータ転送ステップと、

上記第１のターミナルサーバにおける上記クライアントパラメータの正当性及び上記第１のチケットデータの行使の有無を検証する検証ステップと、

上記クライアントパラメータを所定の規則で符号化した第２のチケットデータを作成する第２チケットデータ作成ステップと、

この第２のチケットデータと上記第１のチケットデータとを照合するチケットデータ照合ステップと、

上記検証ステップ及び上記チケットデータ照合ステップにおける結果に基づいて、上記第２のターミナルサーバへ上記クライアントの接続可否を指示する第２の認証ステップとを備えていることを特徴とするアクセス認証方法。

【請求項７】

第１のターミナルサーバを経由してクライアントに第２のターミナルサーバへの接続サービスを行うアクセス認証システムにおいて、

上記第１のターミナルサーバに対して上記クライアントから入力されたＩＤ及びパスワードに基づいて上記第１のターミナルサーバへの上記クライアントの接続の可否を認証するとともに、上記ＩＤ、上記クライアントのアクセス元ＩＰアドレス、所定の有効期限、共通の文字列からなるクライアントパラメータを所定の規則で符号化した第１のチケットデータを作成し、上記第２のターミナルサー

バに転送する第１の認証サーバと、

上記第２のターミナルサーバに対して上記クライアントから入力されたアクセス元ＩＰアドレスと上記クライアントパラメータのアクセス元ＩＰアドレスとを照合し、上記有効期限内のアクセスであるか否かを判断し、上記第１のチケットデータの行使の有無を判断し、上記クライアントパラメータを上記所定の規則で符号化した第２のチケットデータを作成し、この第２のチケットデータと上記第１のチケットデータとを照合することで、上記第２のターミナルサーバへ上記クライアントの接続可否を指示する第２の認証サーバとを備えていることを特徴とするアクセス認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、所定のアプリケーションプロバイダへのアクセス権を予め有するユーザが異なるアプリケーションプロバイダへのアクセス権を得るためのアクセス認証システム及びアクセス認証方法に関する。

【０００２】

【従来の技術】

ユーザはインターネットを介して様々な情報サービス等の各種サービスを提供するサービス提供者を利用することができる。サービス提供者とは、インターネットを介して接続されたクライアント端末に対してデータやコンテンツを提供したり、情報処理サービスを提供する業者を指している。サービス提供者はそれぞれ独立しており、ユーザは利用したいサービス提供者と契約し、それぞれＩＤとパスワードを持つことでアクセス権を得るようにしている。

【０００３】

【発明が解決しようとする課題】

しかし、サービス提供者は増えており、ユーザがそれぞれのサービス提供者と契約するのはＩＤやパスワードを管理する上で煩雑であった。また、各サービス提供者が提供できるサービスの種類には限界があった。

【０００４】

一方、一つのＩＤとパスワードを複数のサービス提供者間で共通化して用いる方法も考えられるが、ＩＤ及びパスワードの両方を各サービス提供者で保持することになるため、課金や秘密保持の点で問題があった。

【０００５】

そこで本発明は、１つのサーバ（サービス提供者）に対しての個人情報（ＩＤ及びパスワード）のみで、各種サービスを提供する他のサーバ（サービス提供者）を個人情報の全てを開示することなく利用することができるようにするためのアクセス認証システム及びアクセス認証方法を提供することを目的としている。

【０００６】

【課題を解決するための手段】

上記課題を解決し目的を達成するために、本発明のアクセス認証システム及びアクセス認証方法は次のように構成されている。

【０００７】

（１）第１のターミナルサーバを経由してクライアントに第２のターミナルサーバへの接続サービスを行うアクセス認証システムにおいて、

上記第１のターミナルサーバに対して上記クライアントから入力された個別情報に基づいて上記第１のターミナルサーバへの上記クライアントの接続の可否を認証するとともに、上記個人情報の一部を含むクライアントパラメータを所定の規則で符号化した第１のチケットデータを作成し、上記第２のターミナルサーバに転送する第１の認証サーバと、

上記クライアントパラメータの正当性及び上記第１のチケットデータの行使の有無を検証するとともに、上記クライアントパラメータを所定の規則で符号化した第２のチケットデータを作成し、この第２のチケットデータと上記第１のチケットデータとを照合し、上記第２のターミナルサーバへ上記クライアントの接続可否を指示する第２の認証サーバとを備えていることを特徴とする。

【０００８】

（２）上記（１）に記載されたアクセス認証システムであって、上記所定の規則は、一方向関数による要約であることを特徴とする。

【０００９】

（３）上記（１）に記載されたアクセス認証システムであって、上記クライアントパラメータには、上記クライアントのＩＤ、アクセス元ＩＰアドレス、上記第１のチケットデータの有効期限のうち少なくとも１つが含められていることを特徴とする。

【００１０】

（４）上記（１）に記載されたアクセス認証システムであって、上記第１及び第２の認証サーバにおいて、上記第１及び第２のチケットデータを作成する際に、予め定められた共通の文字列を含めることを特徴とする。

【００１１】

（５）上記（４）に記載されたアクセス認証システムであって、上記共通の文字列は、所定のタイミングで変更されるものであることを特徴とする。

【００１２】

（６）第１のターミナルサーバを経由してクライアントに第２のターミナルサーバへの接続サービスを行うアクセス認証方法において、上記第１のターミナルサーバへの上記クライアントの接続の可否を認証する第１の認証ステップと、上記クライアントから入力された個別情報の少なくとも一部を含むクライアントパラメータを所定の規則で符号化した第１のチケットデータを作成する第１チケットデータ作成ステップと、上記第２のターミナルサーバに上記クライアントパラメータ及び上記第１のチケットデータを転送するデータ転送ステップと、上記第１のターミナルサーバにおける上記クライアントパラメータの正当性及び上記第１のチケットデータの行使の有無を検証する検証ステップと、上記クライアントパラメータを所定の規則で符号化した第２のチケットデータを作成する第２チケットデータ作成ステップと、この第２のチケットデータと上記第１のチケットデータとを照合するチケットデータ照合ステップと、上記検証ステップ及び上記チケットデータ照合ステップにおける結果に基づいて、上記第２のターミナルサーバへ上記クライアントの接続可否を指示する第２の認証ステップとを備えていることを特徴とする。

【００１３】

（７）第１のターミナルサーバを経由してクライアントに第２のターミナルサー

バへの接続サービスを行うアクセス認証システムにおいて、上記第１のターミナルサーバに対して上記クライアントから入力されたＩＤ及びパスワードに基づいて上記第１のターミナルサーバへの上記クライアントの接続の可否を認証するとともに、上記ＩＤ、上記クライアントのアクセス元ＩＰアドレス、所定の有効期限、共通の文字列からなるクライアントパラメータを所定の規則で符号化した第１のチケットデータを作成し、上記第２のターミナルサーバに転送する第１の認証サーバと、上記第２のターミナルサーバに対して上記クライアントから入力されたアクセス元ＩＰアドレスと上記クライアントパラメータのアクセス元ＩＰアドレスとを照合し、上記有効期限内のアクセスであるか否かを判断し、上記第１のチケットデータの行使の有無を判断し、上記クライアントパラメータを上記所定の規則で符号化した第２のチケットデータを作成し、この第２のチケットデータと上記第１のチケットデータとを照合することで、上記第２のターミナルサーバへ上記クライアントの接続可否を指示する第２の認証サーバとを備えていることを特徴とする。

【００１４】

【発明の実施の形態】

図１は本発明の一実施の形態に係るアクセス認証システムの構成を示す図、図２の（ａ），（ｂ）は同アクセス認証システムに組み込まれた認証サーバ２２，３２の構成を示すブロック図、図３はアクセス認証の手順を示すフロー図である。なお、本実施の形態はソフトウエア処理により実現する場合も含まれる。

【００１５】

図１中１０はユーザのクライアント端末、２０はユーザと契約関係にあるサービス提供先サービス提供者、３０はユーザと直接の契約関係にないサービス提供元サービス提供者、４０はインターネット回線、５０は電話回線を示している。

【００１６】

サービス提供先サービス提供者２０は、インターネット回線４０に接続されたターミナルサーバ（第１のターミナルサーバ）２１と、このターミナルサーバ２１に接続され後述するような認証等を行う認証サーバ（第１の認証サーバ）２２と、ターミナルサーバ２２に接続されるとともに情報サービスを提供するメイン

サーバ２３と、電話回線５０に接続された共通の文字列更新部２４とを備えている。

【００１７】

認証サーバ２２は、第１のターミナルサーバ２１に対してクライアント端末１０から入力されたＩＤ及びパスワードに基づいてターミナルサーバ２１のへのクライアント端末１０からの接続の可否を認証する認証部２２ａと、クライアント端末１０のアクセス元ＩＰアドレスを検出するＩＰアドレス検出部２２ｂと、後述する第１チケット（第１のチケットデータ）の有効期限を生成する有効期限生成部２２ｃと、クライアントパラメータＰ、すなわちＩＤ、クライアントのアクセス元ＩＰアドレス、有効期限生成部２２ｃで生成された有効期限、共通の文字列更新部２４で更新された最新の共通の文字列を一方向関数で要約する等の所定の規則を用いて第１チケットデータＤ１を作成するチケットデータ生成部２２ｄと、クライアントパラメータＰ及び第１チケットデータを認証サーバ３２にインターネット回線４０及びターミナルサーバ３１を介して転送する転送部２２ｅとを備えている。

【００１８】

サービス提供元サービス提供者３０は、インターネット回線４０に接続されたターミナルサーバ（第２のターミナルサーバ）３１と、このターミナルサーバ３１に接続され後述するような認証等を行う認証サーバ（第２の認証サーバ）３２と、ターミナルサーバ３１に接続されるとともに情報サービスを提供するメインサーバ３３と、電話回線５０に接続された共通の文字列更新部３４とを備えている。

【００１９】

認証サーバ３２は、ターミナルサーバ３１に対してクライアント端末１０から入力されたアクセス元ＩＰアドレスと上述した認証サーバ２２から転送されたクライアントパラメータＰのアクセス元ＩＰアドレスとを照合するアクセス元ＩＰアドレス照合部３２ａと、有効期限内のアクセスであるか否かを判断する有効期限判断部３２ｂと、第１のチケットデータＤ１の行使の有無を判断するチケット行使判断部３２ｃと、転送されたクライアントパラメータＰを上述した規則と同

一の規則で符号化した第２のチケットデータＤ２を作成するチケットデータ生成部３２ｄと、第２のチケットデータＤ２と第１のチケットデータＤ１とを照合することで、第２のターミナルサーバ３１へクライアント端末１０からの接続可否を指示する認証部３２ｅとを備えている。

【００２０】

共通の文字列更新部２４及び共通の文字列更新部３４は、文字列から構成される同一の共通の文字列を保持しており、定期的に更新されている。

【００２１】

このように構成されていると、ユーザがクライアント端末１０からメインサーバ３３にアクセスする場合には次のように行われる。すなわち、ユーザはクライアント端末１０からインターネット回線４０を介してターミナルサーバ２１に接続を行う。このとき、ユーザはサービス提供先サービス提供者が提供するログイン画面に自己のＩＤ及びパスワードを入力する（ＳＴ１０）。このとき、ターミナルサーバ２１では、任意のアクセス制限を行い（ＳＴ１１）、アクセスが禁止された場合にはログインが拒否される（ＳＴ１２）。

【００２２】

ＳＴ２においてアクセスが許可された場合には、ＩＤ、パスワード、アクセス元ＩＰアドレスが認証サーバ２２に送られ、認証部２２ａにてＩＤ及びパスワードに基づいてユーザ認証を行い（ＳＴ１３）、認証に失敗した場合にはログインが拒否される（ＳＴ１４）。なお、この時点でメインサーバ２３へのアクセスが許可される。

【００２３】

ＳＴ４においてユーザ認証が成功した場合には、ＩＰアドレス検出部２２ｂにおいてクライアント端末１０のアクセス元ＩＰアドレスが検出され、有効期限生成部２２ｃにおいて第１チケットデータＤ１の有効期限を生成する。そして、チケットデータ生成部２２ｄにおいて、クライアントパラメータＰ（ＩＤ、アクセス元ＩＰアドレス、有効期限、共通の文字列）を一方向関数で要約して第１チケットデータＤ１を作成する（ＳＴ１５）。

【００２４】

次に、転送部２２ｅによりクライアントパラメータＰ及び第１チケットデータＤ１を認証サーバ３２にインターネット回線４０及びターミナルサーバ３１を介して転送する（ＳＴ１６）。

【００２５】

サービス提供元サービス提供者３０の認証サーバ３２では、アクセス元ＩＰアドレス照合部３２ａによりアクセス元ＩＰアドレス照合部３２ａターミナルサーバ３１に対してクライアント端末１０から入力されたアクセス元ＩＰアドレスと上述した認証サーバ２２から転送されたクライアントパラメータＰのアクセス元ＩＰアドレスとを照合し（ＳＴ２０）、不一致である場合にはログインは拒否される（ＳＴ２１）。

【００２６】

次に、有効期限判断部３２ｂにより、有効期限内のアクセスであるか否かを判断し（ＳＴ２２）、有効期限を経過している場合には無効とされログインは拒否される（ＳＴ２３）。

【００２７】

次に、チケット行使判断部３２ｃにより、第１のチケットデータＤ１の行使の有無を判断し（ＳＴ２４）、既に行使されている場合にはログインは拒否される（ＳＴ２５）。

【００２８】

次に、チケットデータ生成部３２ｄにより、転送されたクライアントパラメータＰを上述した一方向関数で要約した第２のチケットデータＤ２を作成し、第１のチケットデータＤ１とを照合し（ＳＴ２６）、不一致の場合にはログインは拒否される（ＳＴ２７）。

【００２９】

次に、ＩＤが既に登録されているものか否かを検索し（ＳＴ２８）、登録されていれば後述するＳＴ３０に進み、登録されていなければＩＤが作成される（ＳＴ２９）。そして、メインサーバ３３へのログインが可能となる（ＳＴ３０）。

【００３０】

なお、このようなアクセス認証システムの場合には、サービス提供先サービス

提供者２０からサービス提供元サービス提供者３０にクライアントパラメータＰが転送される際に、何らかの方法でクライアントパラメータＰを傍受し、クライアントパラメータＰを改竄して不正アクセスしようとしても、第１のチケットデータＤ１と改竄されたクライアントパラメータＰに基づいて作成された第２のチケットデータＤ２とが不一致となり、ログインが拒否されることになる。

【００３１】

なお、改竄されたクライアントパラメータＰに基づいて第１のチケットデータＤ１を作ることにより、新たなサービス提供元サービス提供者３０へのログインが可能になる。しかしながら、第１のチケットデータＤ１の作成には共通の文字列を知る必要がある。しかも、この共通の文字列は、認証サーバ２２，３２に侵入して入手したり、総当たり法によって推測したり、一方向関数の逆演算して導き出すことが考えられるが、共通の文字列の更新を十分に短く設定することで、事実上共通の文字列を入手することが困難になる。

【００３２】

また、クライアントパラメータＰ及び第１のチケットデータＤ１を流用しようとしても、有効期限を十分に短く設定しておけば、有効期限後のアクセスとなる可能性が高く、ログインが拒否されることになる。

【００３３】

さらに、有効期限内の使用であっても、正規のユーザによるサービス提供元サービス提供者３０へのアクセスは、サービス提供先サービス提供者２０へのアクセスとほぼ同時である。このため、クライアントパラメータＰ及び第１のチケットデータＤ１を第三者が傍受し不正使用しようとしても、既に正規のユーザによって第１のチケットデータＤ１の行使が済んでおり、第三者の第１のチケットデータＤ１ではログインができない。

【００３４】

一方、正規なユーザが共通の文字列を含んだ状態で生成された第１のチケットデータＤ１をサービス提供元サービス提供者３０に到達した時点で、共通の文字列が更新されていて第２のチケットデータＤ２と第１のチケットデータＤ１が異なってしまいログインが拒絶されてしまう問題は、次のようにして解決する。

【００３５】

例えば、定期的にＡ，Ｂ，Ｃ，Ｄという順番で共通の文字列を変える場合、ＡＢ，ＢＣ，ＣＤ，…というように２つの共通の文字列を組み合わせることで、２種類の第１のチケットデータＤ１を作成し、この２つの第１のチケットデータＤ１のいずれかが第２のチケットデータＤ２と一致すればログイン可能とするように設定することにより対処する。

【００３６】

上述したように、本発明の一実施の形態に係るアクセス認証システムによれば、１つのサービス提供先サービス提供者に対してのＩＤ及びパスワードのみで、各種サービスを提供する他のサービス提供元サービス提供者にパスワードを開示することなく利用することが可能となる。また、サービス提供先サービス提供者からサービス提供元サービス提供者に転送されるデータが第三者により傍受された場合であっても、何重にも安全対策が講じられているため、サービス提供元サービス提供者に不正にアクセスがされることがない。

【００３７】

なお、本発明は前記実施の形態に限定されるものではなく、本発明の要旨を逸脱しない範囲で種々変形実施可能であるのは勿論である。

【００３８】

【発明の効果】

本発明によれば、１つのサーバ（サービス提供者）に対しての個人情報（ＩＤ及びパスワード）のみで、各種サービスを提供する他のサーバ（サービス提供者）を個人情報の全てを開示することなく利用することが可能となる。

【図面の簡単な説明】

【図１】

本発明の一実施の形態に係るアクセス認証システムの構成を示す図。

【図２】

同アクセス認証システムに組み込まれた認証サーバの構成を示すブロック図。

【図３】

同アクセス認証システムの動作を示すフロー図。

【符号の説明】

１０…クライアント端末

２０…サービス提供先サービス提供者

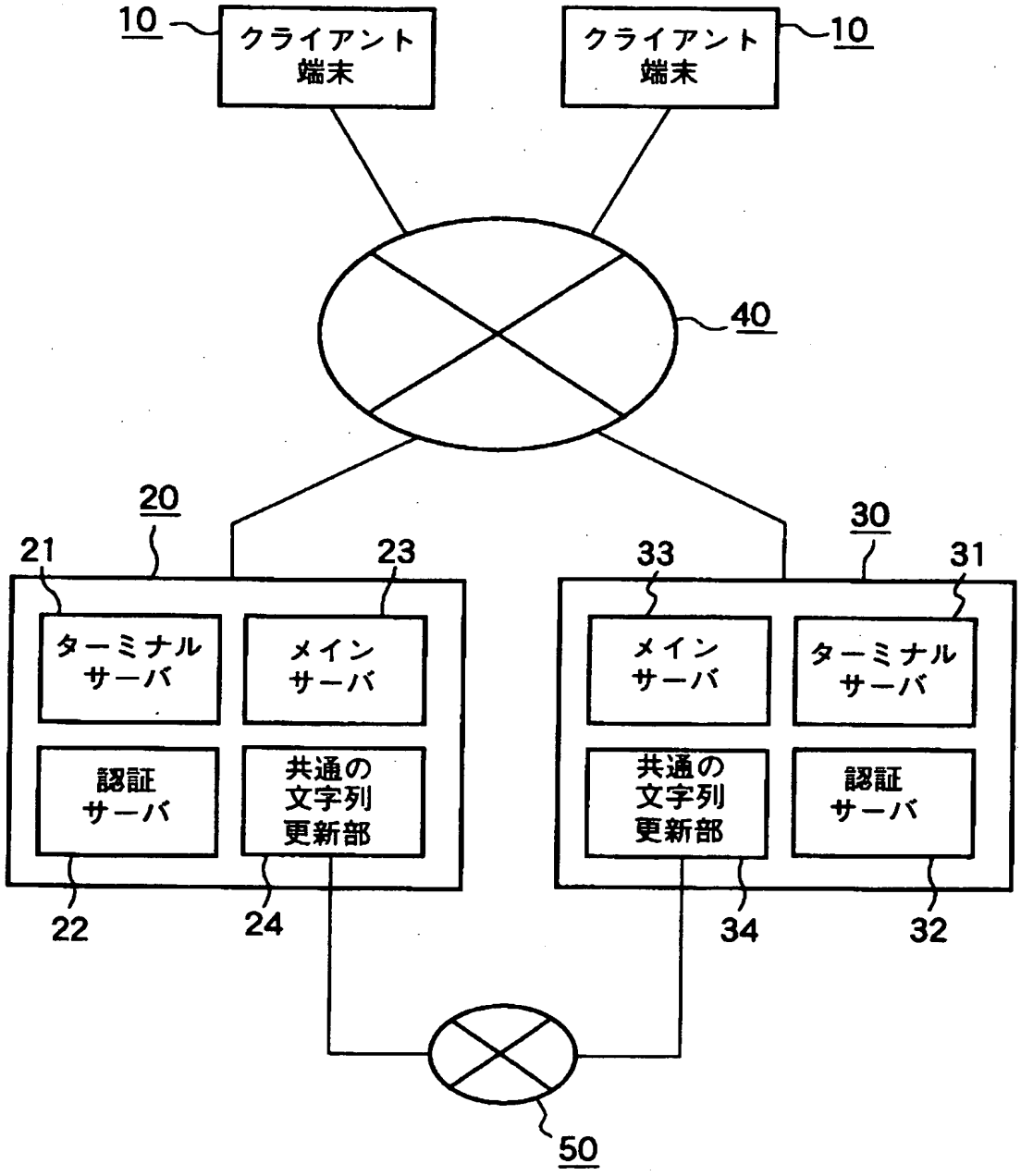
３０…サービス提供元サービス提供者

４０…インターネット回線

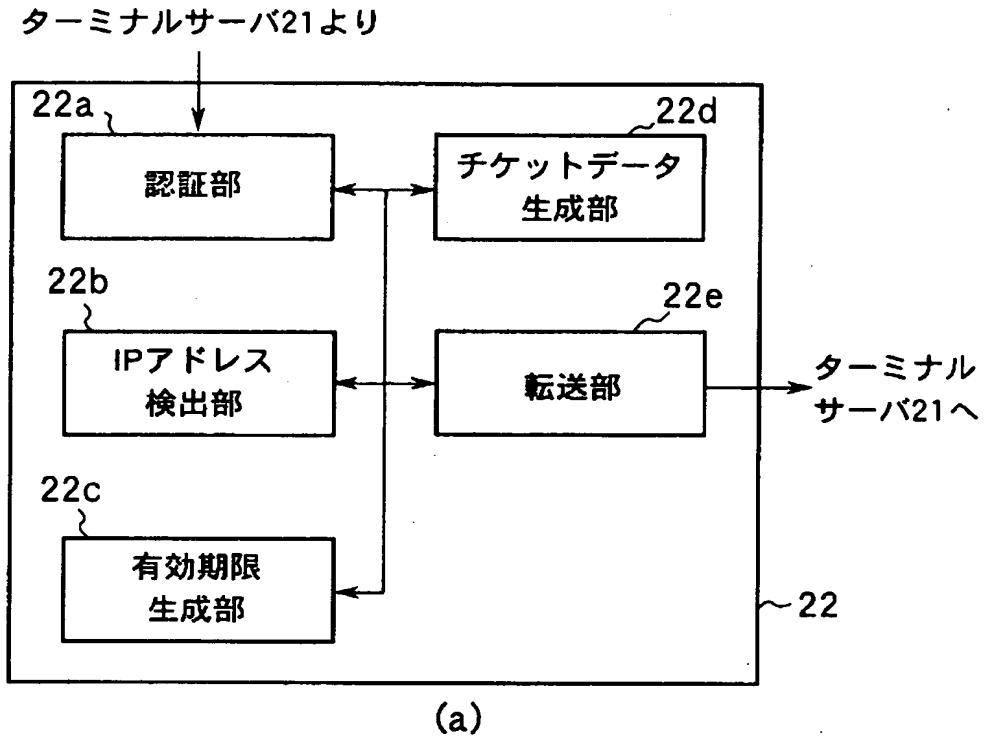
５０…電話回線

【書類名】　図面

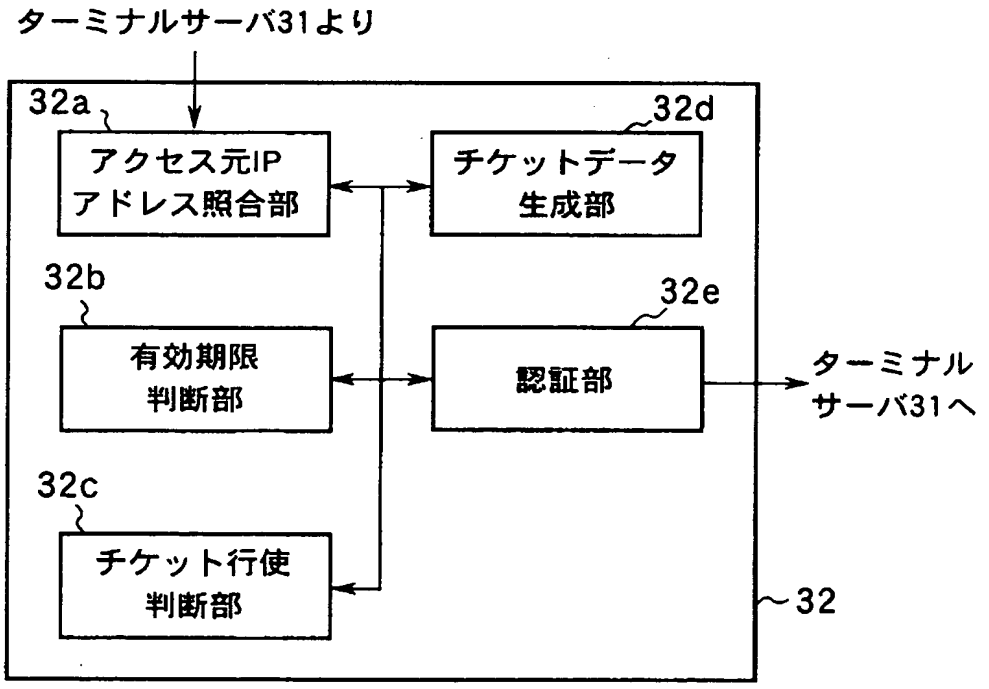
【図１】


10
クライアント端末
クライアント端末
10
40
20
21
23
30
33
31
ターミナルサーバ
メインサーバ
メインサーバ
ターミナルサーバ
認証サーバ
共通の文字列更新部
共通の文字列更新部
認証サーバ
22
24
34
32
50

【図２】

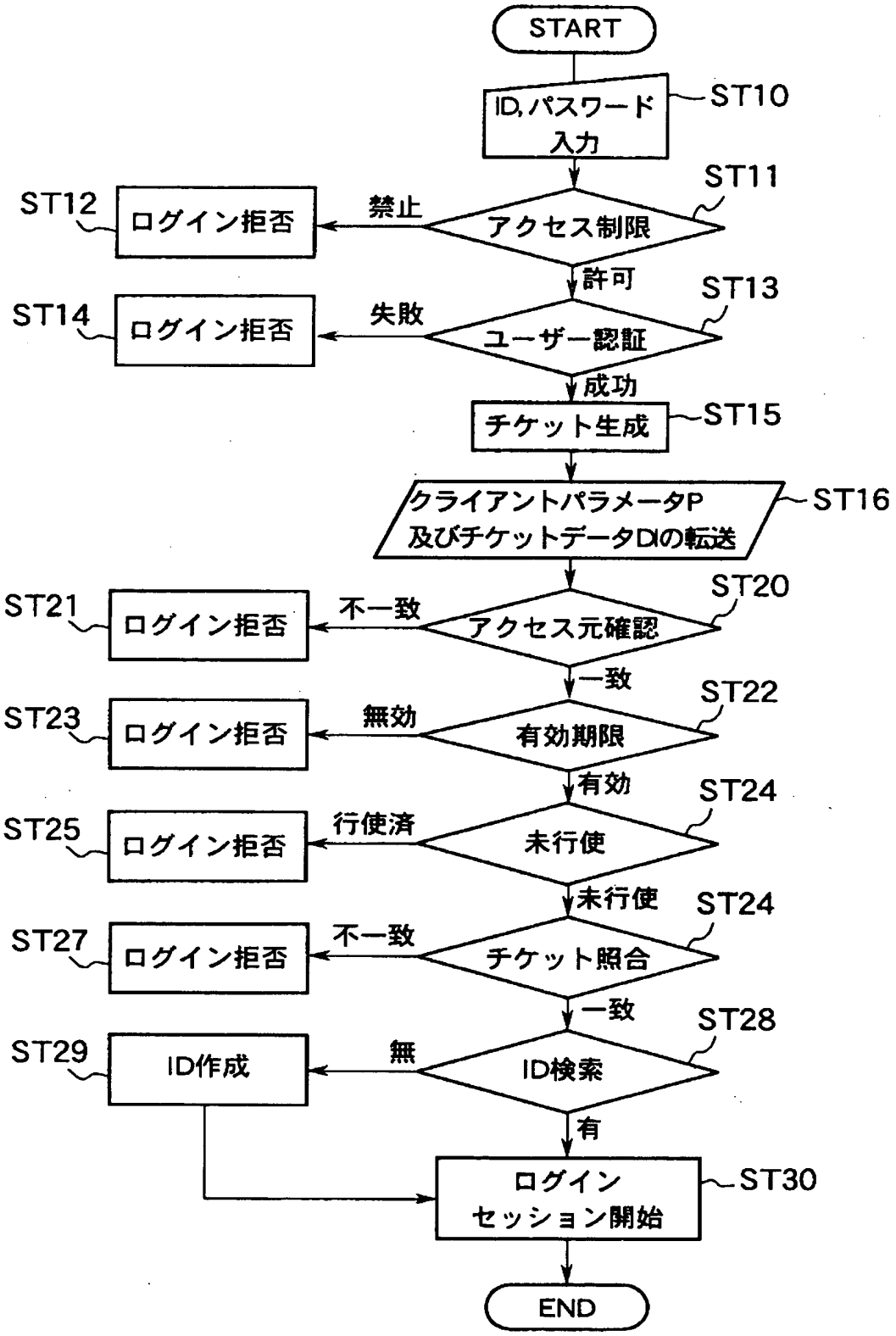

ターミナルサーバ21より
22a
認証部
22d
チケットデータ
生成部
22b
IPアドレス
検出部
22e
転送部
ターミナル
サーバ21へ
22c
有効期限
生成部
22

(a)


ターミナルサーバ31より
32a
アクセス元IP
アドレス照合部
32d
チケットデータ
生成部
32b
有効期限
判断部
32e
認証部
ターミナル
サーバ31へ
32c
チケット行使
判断部
32

(b)

【図３】


START
ID,パスワード入力
ST10
ST11
アクセス制限
禁止
ST12
ログイン拒否
許可
ST13
ユーザー認証
失敗
ST14
ログイン拒否
成功
チケット生成
ST15
クライアントパラメータP及びチケットデータDIの転送
ST16
ST20
アクセス元確認
不一致
ST21
ログイン拒否
一致
ST22
有効期限
無効
ST23
ログイン拒否
有効
ST24
未行使
行使済
ST25
ログイン拒否
未行使
ST24
チケット照合
不一致
ST27
ログイン拒否
一致
ST28
ID検索
無
ST29
ID作成
有
ログインセッション開始
ST30
END

【書類名】　　要約書

【要約】

【課題】１つのサーバに対しての個人情報に基づいて、各種サービスを提供する他のサーバを利用可能とするアクセス認証システムを提供すること。

【解決手段】クライアント端末１０から入力された個別情報に基づいて第１のターミナルサーバへの接続の可否を認証するとともに、クライアントパラメータＰを符号化した第１のチケットデータを作成し、第２のターミナルサーバに転送する第１の認証サーバ２２と、クライアントパラメータＰの正当性及び第１のチケットデータＤ１の行使の有無を検証するとともに、クライアントパラメータＰを符号化した第２のチケットデータＤ２を作成し、第２のチケットデータＤ２と第１のチケットデータＤ１とを照合し、第２のターミナルサーバ３１へクライアント端末１０の接続可否を指示する第２の認証サーバ３２とを備えている。

【選択図】　　図１

【書類名】　出願人名義変更届（一般承継）
【整理番号】　AK00001028
【提出日】　平成12年11月29日
【あて先】　特許庁長官　殿
【事件の表示】
　【出願番号】　特願2000- 69079
【承継人】
　【識別番号】　500257300
　【氏名又は名称】　ヤフー株式会社
【承継人代理人】
　【識別番号】　100058479
　【弁理士】
　【氏名又は名称】　鈴江　武彦
　【電話番号】　03-3502-3181
【提出物件の目録】
　【物件名】　権利の承継を証明する書面　1
　【提出物件の特記事項】　手続補足書に添付して提出する。
　【包括委任状番号】　0017007
【プルーフの要否】　要

認定・付加情報

特許出願の番号	特願２０００－０６９０７９
受付番号	５００００１５３６４６９
書類名	出願人名義変更届（一般承継）
担当官	濱谷　よし子　　１６１４
作成日	平成１３年　３月　８日

＜認定情報・付加情報＞

【承継人】

【識別番号】	500257300
【住所又は居所】	東京都港区北青山３－６－７
【氏名又は名称】	ヤフー株式会社

【承継人代理人】　申請人

【識別番号】	100058479
【住所又は居所】	東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許法律事務所内
【氏名又は名称】	鈴江　武彦

次頁無

出　願　人　履　歴　情　報

識別番号　　〔５００１１２２５０〕

１．変更年月日　　２０００年　３月１３日
［変更理由］　新規登録
住　所　兵庫県神戸市中央区港島南町１－５－２
氏　名　ピー・アイ・エム株式会社

２．変更年月日　　２０００年１１月２７日
［変更理由］　住所変更
住　所　東京都渋谷区恵比寿一丁目２４番１６号
氏　名　ピー・アイ・エム株式会社

出　願　人　履　歴　情　報

識別番号　　〔５００２５７３００〕

１．変更年月日　　２０００年　６月　２日
［変更理由］　新規登録
住　所　　東京都港区北青山３－６－７
氏　名　　ヤフー株式会社